Exhibit 9

Expand All

VMware NSX Product Documentation

- NSX Administration Guide
  - NSX Manager
  - Tier-0 Gateways
  - Tier-1 Gateway
  - Segments
  - DHCP
  - Host Switches
  - Virtual Private Network (VPN)
  - Network Address Translation (NAT)
  - NSX Advanced Load Balancer (Avi)
  - Load Balancer
  - Distributed Load Balancer
  - Ethernet VPN (EVPN)
  - Forwarding Policies
  - IP Address Management (IPAM)
  - Networking Settings
  - Security
    - Firewall Rule Enforcement
    - Security Overview
    - NSX Guest Introspection Platform
    - Security Monitoring
    - Security Terminology
    - Identity Firewall
    - Layer 7 Context Profile

Monitoring IDS/IPS Events

Updated on 10/19/2022

Selected product version: VMware NSX 4.1

You can monitor events and view data of the last 14 days.

To view intrusion events, navigate to **Security > (and then) IDS/IPS** . You can filter the events based on the following criteria:

- Filter criteria. Select from the following options:

Filter Criteria	Description
Attack Target	Target of the attack.
Attack Type	Type of attack, such as trojan horse, or denial of service (DoS).
CVSS	Common Vulnerability Score (filter based on a score above a set threshold).
Gateway Name	The gateway name on which the event was registered.
IP Address	IP address on which the event was registered.
Product Affected	Vulnerable product or (version), such as Windows XP or Web_Browsers.
Signature ID	Unique ID of the signature rule.
VM Name	The VM (based on logical port) on which the event was registered.

- Traffic: Select from the following options:
  - All traffic
  - Distributed only
  - Gateway only
- Signature actions: Select from the following options:
  - Show all signatures
  - Dropped (Prevented)
  - Rejected (Prevented)
  - Alert (Detect Only)
- Severity rating: Select from the following options:
  - Critical
  - High
  - Medium
  - Low
  - Suspicious

You can toggle the **Timeline** button to view or hide the timeline graph that is based on severity ratings. The graph presents events that occurred over a selected time span. You can zoom in to the specific time window on this graph to view details of signatures of the related events that happened during the time window.

On the timeline graph, colored dots indicate the unique type of intrusion events and can be clicked for details. The size of the dot indicates the number of times an intrusion event has been seen. A blinking dot indicates that an attack is ongoing. Point to a dot to see the attack name, number of attempts, first occurrence, and other details.

- Red dots - represent critical severity signature events.
- Orange dots - represent high severity signature events.
- Yellow dots - represent medium severity signature events.
- Gray dots - represent low severity signature events.
- Purple - represent suspicious severity signature events.

All the intrusion attempts for a particular signature are grouped and plotted at their first occurrence.

Click the arrow next to an event to view details.

Detail	Description
Impact Score	Impact score is a combined value of risk score (the severity of the threat) and the confidence score (strength of the detection being correct).
Severity	Signature severity of the intrusion.
Last Detected	This is the last time the signature was fired.
Details	Brief description of what the signature is targeting.
Users Affected	Number of users who were impacted by the event.
Workloads	Number of workloads affected. Click to view affected workload details.
CVE Details	CVE reference of the vulnerability targeted by the exploit.
CVSS	Common Vulnerability Score of the vulnerability targeted by the exploit.
Intrusion Event Details (latest occurrence) - Source	IP address of the attacker and source port used.
Intrusion Event Details (latest occurrence) - Gateway	Edge node details that contain the workload on which the event was registered.
Intrusion Event Details (latest occurrence) - Hypervisor	Transport node details that contain the workload on which the event was registered.
Intrusion Event Details (latest occurrence) - Target	IP address of the victim and destination port used.
Attack Direction	Client-Server or Server-Client.
Attack Target	Target of the attack.
Attack Type	Type of attack, such as trojan horse, or denial of service (DoS).
Product Affected	Illustrates what product is vulnerable to the exploit.
Total Events	Total number of intrusion attempts for the event.

Intrusion Activity	Displays the total number of times this particular IDS signature was triggered, the most recent occurrence, and the first occurrence.
Service	Protocol information associated with the event.
Signature ID	Unique ID of the IDS signature.
Signature Revision	The revision number of the IDS signature.
Mitre Technique	MITRE ATT&CK technique describing the detected activity.
Mitre Tactic	MITRE ATT&CK tactic describing the detected activity.
Associated IDS Rule	Clickable link to the configured IDS Rule which resulted in this event.

To view full intrusion history, click the **View Full Event History** link. A window opens with the following details:

Detail	Description
Time Detected	This is the last time the signature was fired.
Traffic Type	This could be Distributed or Gateway. Distributed indicates East-West traffic flow and Gateway indicates North-South traffic flow.
Workloads/IPs Affected	Number of virtual machines or IP addresses which has hit the given attack or vulnerability for a given traffic flow.
Attempts	Number of intrusion attempts made for an attack or vulnerability during a given traffic flow.
Source	IP address of the attacker.
Destination	IP address of the victim.
Protocol	Traffic protocol of the detected intrusion.
Rule	Rule to which the signature belongs (through the profile).
Profile	Profile to which the signature belongs.
Action	Any of the following actions that was triggered against the event: ▪ Drop ▪ Reject ▪ Alert

You can also filter intrusion history based on the following criteria:

- Action
- Destination IP
- Destination Port
- Protocol
- Rule
- Source IP
- Source Port
- Traffic Type

Remote logging

Remote logging

NSX components write to log files in the directory `/var/log`. On NSX appliances, NSX syslog messages conform with RFC 5424. On ESXi hosts, syslog messages conform with RFC 3164.

There are three event log files in the `/var/log/nsx-idps` folder on ESXi hosts:

- fast log - Contains internal logging of nsx-idps process events, with limited information and is used only for debugging purposes.
- nsx-idps-log - Contains general nsx-idps process logs with basic information and errors about the process workflow.
- nsx-idps-events.log - Contains detailed information about events (all alerts/drops/rejects) with NSX metadata.

To enable the sending of NSX IDS/IPS logs to a central log repository, use the following APIs.

Run the following API to query the current settings.

`GET https://<Manager-IP>/api/v1/global-configs/IdsGlobalConfig`

```
{
   ...
   "global_idsevents_to_syslog_enabled": false,
   ...
 }
```

If the *global_idsevents_to_syslog.enabled* variable is set to false, run the following API to set it to true.

`PUT https://<Manager-IP>/api/v1/global-configs/IdsGlobalConfig`

```
Result:
    {
      "global_idsevents_to_syslog_enabled": true,
      "_revision": <revision number from GET>
     }
```

These events are exported directly from ESXi hosts so ensure remote syslog is configured on the ESXi host.

You must also ensure that the NSX manager and ESXi hosts are also setup to forward syslog messages to the central log repository.

For more information about configuring remote logging, see Configure Remote Logging and all related information under the section Log Messages and Error Codes.

Parent topic: NSX IDS/IPS and NSX Malware Prevention

« Previous Page Next Page »